What is claimed is:

1. A method of detecting decryption of encrypted viral code in a subject file, comprising:

emulating computer executable code in a subject file;

flagging a memory area that is read during emulation of a first instruction in the computer executable code; and

detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code.

2. A method of detecting encrypted viral code in a subject file, comprising:

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified memory area; and

triggering a viral detection alarm, if one of the listed memory regions is larger than a predetermined size.

3. The method of claim 2, wherein the emulation is performed on an instruction-by-instruction basis.

4. The method of claim 2, further comprising:

determining whether a selected one of the listed memory regions overlaps the modified memory area; and

updating the selected memory region to encompass the modified memory area.

5. The method of claim 2, further comprising:

determining whether a selected one of the listed memory regions is contiguous

with the modified memory area; and

updating the selected memory region to encompass the modified memory area.

6. The method of claim 2, further comprising:

determining whether the modified memory area overlaps the listed memory regions; and

adding the modified memory area as a new memory region to the list of memory regions, if the modified memory area does not overlap any of the listed memory regions.

7. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting decryption of encrypted viral code in a subject file, the method steps comprising:

emulating computer executable code in a subject file;

flagging a memory area that is read during emulation of a first instruction in the computer executable code; and

detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code.

8. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for detecting encrypted viral code in a subject file, the method steps comprising:

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified memory area; and

triggering a viral detection alarm, if one of the listed memory regions is larger

than a predetermined size.

9. A computer system, comprising:

a processor; and

a program storage device readable by the computer system, tangibly embodying a program of instructions executable by the processor to perform method steps for detecting decryption of encrypted viral code in a subject file, the method steps including

emulating computer executable code in a subject file;

flagging a memory area that is read during emulation of a first instruction in the computer executable code; and

detecting a modification to the flagged memory area during emulation of a second instruction in the computer executable code.

10. A computer system, comprising:

a processor; and

a program storage device readable by the computer system, tangibly embodying a program of instructions executable by the computer system to perform method steps for detecting encrypted viral code, the method steps including

emulating computer executable code in a subject file;

maintaining a list of memory regions that have been read and then modified during the emulation;

determining whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code;

updating the list of memory regions to include the modified memory area; and

triggering a viral detection alarm, if one of the listed memory regions is larger than a predetermined size.

11. An apparatus for detecting decryption of encrypted viral code in a subject file,

comprising:

a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, flags a memory area that is read during the emulation of a first instruction in the computer executable code, and detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code.

12. An apparatus for detecting encrypted viral code in a subject file, comprising:

a code emulator, wherein the code emulator emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a memory monitor, wherein the memory monitor monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory area, and triggers a viral detection alarm, if one of the listed memory regions is larger than a predetermined size.

13. The apparatus of claim 12, wherein the code emulator performs the emulation on an instruction-by-instruction basis.

14. The apparatus of claim 12, wherein the memory monitor determines whether a selected one of the listed memory regions overlaps the modified memory area, and updates the selected memory region to encompass the modified memory area.

15. The apparatus of claim 12, wherein the memory monitor determines whether a selected one of the listed memory regions is contiguous with the modified memory area, and updates the selected memory region to encompass the modified memory area.

16. The apparatus of claim 12, wherein the memory monitor determines whether the modified memory area does not overlap the listed memory regions, and adds the modified memory area as a new memory region to the list of memory regions.

17. A computer data signal embodied in a transmission medium which embodies instructions executable by a computer for detecting decryption of encrypted viral code in a subject file, comprising:

a first segment including emulator code, wherein the emulator code emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a second segment including memory monitor code, wherein the memory monitor code monitors the memory access information output by the code emulator, flags a memory area that is read during the emulation of a first instruction in the computer executable code, and detects a modification to the flagged memory area during emulation of a second instruction in the computer executable code.

18. A computer data signal embodied in a transmission medium which embodies instructions executable by a computer for detecting encrypted viral code in a subject file, comprising:

a first segment including emulator code, wherein the emulator code emulates computer executable code in a subject file, and outputs memory access information corresponding to the emulated computer executable code; and

a second segment including memory monitor code, wherein the memory monitor code monitors the memory access information output by the code emulator, maintains a list of memory regions that have been read and modified during emulation, determines whether a memory area is read during emulation of a first instruction in the computer

executable code and whether the memory area is modified during emulation of a second instruction in the computer executable code, updates the list of memory regions to include the modified memory area, and triggers a viral detection alarm, if one of the listed memory regions is larger than a predetermined size.